REMARKS

The Applicants request reconsideration of the rejection.

Claims 22-24 are pending, claims 1-21 having been canceled without prejudice.

New claims 22-24 are believed to avoid the informalities cited by the Examiner on pages 2-3 of the Office Action.

Further, new claims 22-24 are distinguishable from Belani, U.S. Patent No. 6,772,350 (Belani), which was cited against the claims, whether taken individually or in combination with any other reference of record.

In particular, new claim 22 recites a server having a storage device and a controller connected to the storage device. The storage device stores access permission setting values of user terminal identification information and of user terminal communication capability information. The storage device further stores vertical relation information indicating a vertical relation between access permission information of the identification information and access permission information of the communication capability information. The vertical relation information indicates that the access permission information of the identification information is in a higher level than that of the access permission information of the communication capability information.

When the access permission setting value of the communication capability information is changed from a not permitted state to a permitted state, the controller sets the access permission setting value of the identification information to a permitted state. On the other hand, when the access permission setting value of the identification information is changed from a permitted state to a not permitted state,

the controller sets the access permission setting value of the communication capability information to a not permitted state.

While Belani is directed to controlling access to resources in a distributed environment, Belani does not disclose or fairly suggest that when an access permission setting value of communication capability information is changed from a not permitted state to a permitted state, the access permission setting value of identification information is set to a permitted state; and when the access permission setting value of the identification information is changed from a permitted state to a not permitted state, the access permission setting value of the communication capability information is set to a not permitted state. More generally, Belani does not disclose or fairly suggest that when an access permission setting value of a higher level first type of information is changed from a not permitted state to a permitted state, the access permission setting value of a lower level second type of information is changed to a permitted state in response to the change of state of the first information setting values, and when the access permission setting value of the lower level second type of information is changed from a permitted state to a not permitted state, the access permission setting value of the higher level first type of information is changed to a not permitted state in response to the change of state of the second information setting values.

Col. 11, lines 50-60 of Belani seem to suggest that a permission value can be automatically inherited from a high level information to a low level information when no permission value was previously set to the low level information. However, this does not comport with the now-claimed requirement for the access permission

setting value to change for one information in response to the access permission setting value changing for the other information.

Dependent claim 23 requires the access permission setting values to include the values for an open operation, a read operation, and a write operation of information to be accessed. The Applicants refer the Examiner, for example, to Fig. 5 and the associated discussion in the present disclosure.

Dependent claim 24 requires the access permission setting values for the open, read, and write operations to have hierarchical levels of access permission setting values, the level of the access permission setting values of the open operation being higher than that of the read operation, and the level of the access permission setting values of the read operation being higher than that of the write operation. Further, claim 24 recites that when the access permission setting values of a lower level operation are changed from not permitted to permitted, the controller sets the access permission setting values of a relatively higher level (compared to the lower level being changed) to a permitted state, and when the access permission setting values of a higher level are changed from permitted to not permitted, the controller sets the access permission setting values of a lower level (compared to the higher level being changed) to a not permitted state.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, the Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to

the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. NIT-415).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

_____

Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120